Wilmington Police Department

Directive: .07.17

Fusus Operations & Public Safety Camera Network

CALEA Standards:

NCLEA Standards:

I. Purpose:

It is the policy of the Wilmington Police Department (WPD) to utilize available camera technology within our Public Safety Camera Network to supplement crime prevention efforts, criminal investigations, and prosecution efforts already in place at the agency. Camera technology will improve officer safety and increase situational awareness. The camera technology serves to improve the delivery of police services within the agency's jurisdiction and contribute to increased public safety for our citizens and visitors.

The Public Safety Camera Network is intended to rapidly identify those committing crimes within the view of the Public Safety Cameras, to deter crime, and to assist in successfully prosecuting those who are committing crimes in the agency's jurisdiction.

The agency shall comply with all Federal, State, and Agency ordinances, laws, and regulations regarding privacy.

II. Definitions:

A. FUSUS – A camera integration platform that allows the monitoring of video feeds from multiple public and privately-owned sources, all in real time.

B. PUBLIC SAFTEY CAMERA NETWORK – Any camera providing access to either live or recorded views that have been integrated within the agency video management system (VMS).

C. AGENCY CAMERAS – Any camera installed and maintained by the WPD. These cameras are accessible via the approved video management system (VMS). Maintenance includes equipment ordering, troubleshooting, repair, and replacement.

D. JURISDICTION CAMERAS – Any camera installed and maintained by any entity or department under the same authority of the agency jurisdiction (other than agency cameras and traffic cameras). These cameras are integrated and accessible to the agency through the approved VMS.

Maintenance includes equipment ordering, troubleshooting, repair, and replacement.

E. TRAFFIC CAMERAS – Traffic cameras refer to those cameras maintained by the City of Wilmington Traffic & Engineering Department. City Traffic & Engineering is responsible for selecting the default home location of the cameras.

F. PRIVATE DONOR CAMERAS – Any camera feed owned and maintained by a private entity and the private entity voluntarily elects to participate in the Public Safety Camera Network by providing access to the public area facing camera feeds. All accessible private donor camera feeds will be further documented by a Memorandum of Agreement and all access and settings will be determined by the private donor.

G. STING CENTER – The STING Center Supervisor shall be a civilian employee of WPD who supervises the sworn and non-sworn personnel assigned to the STING Center. The STING Center is responsible for oversight of the Public Safety Camera Network.

H. AGENCY CAMERA TECHNICIAN – A designated camera technician shall be responsible for the maintenance and installation of the AGENCY cameras. Vendor cameras shall be maintained and installed by vendor camera technicians.

I. VOLUNTEER REGISTRY – Instead of providing access, private citizens and business owners with recorded surveillance equipment can volunteer to provide their location and contact information via a registry. Should an incident occur in the area where private surveillance equipment exists, the registry would provide potential evidence of locations and contact information to inquire if a recorded video exists.

III. Agency Camera Locations:

A. Agency cameras shall never be installed in a location where there is a reasonable expectation of privacy.

B. CAMERA LOCATIONS

1. Agency cameras should be placed in areas based on security analysis, the specific needs of the agency, and relevant crime trends. The location of agency cameras is exempt from public records. To protect the integrity of the system, employees shall not include exact location of the cameras within their reports.

2. Camera locations are visible to employees on the approved map-based VMS. Unless otherwise required by the evidence policy, by court order, or by law, agency camera recordings shall be retained for thirty (30)

days and shall then be automatically overwritten. It is the responsibility of those who may need a video to make a request to the STING Center in this time frame.

C. ADDITIONAL CAMERA LOCATIONS

1. Any request or recommendation to have a camera added at a location within the agency's jurisdiction will be made in writing to the STING Center via email, for consideration. If available, temporary overt/covert agency cameras can be deployed for investigative purposes. Any requests should be made to the STING Center Unit Supervisor via the requestor's chain of command.

IV. Camera Monitoring and Operations

A. PUBLIC SAFETY CAMERA NETWORK

1. The STING Center shall have oversight responsibility for the Public Safety Camera Network. Specific responsibilities will be dependent on whether a camera is an agency camera, jurisdiction camera, traffic camera, or private donor camera. Monitoring will take place in the STING Center at the agency. There may be instances when special events, emergency operations, or special details require personnel to monitor the Public Safety Camera Network from remote locations.

B. MONITORING/OPERATING AGENCY CAMERAS

1. STING Center staff shall monitor agency cameras and may operate them at any time when deemed appropriate to assist with an active call for service, special detail, or specifically requested assistance. The STING Center staff may proactively operate jurisdiction cameras if a camera is in a location that would assist STING Center operations. The STING Center staff may review footage for potential evidence that is captured in any jurisdiction camera related to a law enforcement incident if such access is available.

C. MONITORING/OPERATING AGENCY JURISDICTION TRAFFIC CAMERAS

1. Most jurisdiction traffic camera networks have a large footprint, within the jurisdiction of the agency, which is a separate network of cameras from the other jurisdiction cameras. A traffic camera may provide a camera view near an active public safety incident. All traffic camera settings shall be assigned by the City of Wilmington Traffic & Engineering Department, including any home settings. A jurisdiction traffic camera may be temporarily moved from its home position by agency STING Center staff if a public safety incident is reportedly occurring in the immediate area. Account access will be provided to

the City of Wilmington Traffic & Engineering Department cameras to access traffic cameras via the agency -approved VMS.

2. The STING Center will only access and view a live video feed from a traffic camera under the following circumstances:

    a. Jurisdiction traffic cameras are connected to a device capable of sharing the feed with the agency
    b. A public safety incident is reportedly occurring in the immediate area of a jurisdiction traffic camera
    c. Routine audits of the Public Safety Camera Network for maintenance and/or approved training

D. MONITORING PRIVATE DONOR CAMERAS

1. Private Donor Camera feeds will not be recorded by the agency. All recorded video footage shall be the property of the private donor. The process by which recorded video is reviewed and shared by the private donor will be at the sole discretion of each private donor.

2. Private donor camera views will not be accessed by the STING Center unless the following exist:

    a. A Memorandum of Understanding exists between the private donor and the WPD.
    b. Agency will only have access to areas where the public has no reasonable expectation of privacy.
    c. The private donor obtains and utilizes specific equipment to enable agency access to their cameras.
    d. The private donor agrees to share any footage for investigative purposes. The agency will not independently save or record video from private donor cameras without donor authorization.
    e. The private donor is responsible to respond to any request from the media or public regarding their cameras. All private donor video is owned by the private donor and is not subject to public records requests.
    f. The agency shall not access a live feed or control private cameras unless related to a public safety incident or routine audits of the Public Safety Camera Network or system maintenance and approved training.

E. STING CENTER STAFFING

1. The STING Center will be managed by the STING Center Supervisor. Staffing of the STING Center will be during the designated hours of operation. The STING Center is staffed by sworn Intelligence Officers and civilian Intelligence Analysts. The STING Center shall maintain a single main phone line that will be answered during designated operating hours. The STING Center shall also maintain a single main electronic mail (email) address where requests can be sent.

F. AGENCY ACCESS TO CAMERA NETWORKS

1. All STING Center personnel will have access to the Public Safety Camera Network in its entirety and operate in the role of administrators.

2. **Sworn employees of the department will be given access to the Public Safety Camera Network through both the web and mobile applications, giving them access to numerous information-sharing features. Employees may view the Public Safety Camera Network cameras for legitimate police purposes only while on duty. Mobile phone users have the option to send and receive direct messages (text and video) with STING Center staff, allow GPS monitoring of the user's location from the STING Center, and live streaming video/audio back to the staff in the STING Center. These features are initiated by the mobile user. Only those employees who have a department issued cell phone will be able to do this. There will be no usage of personally owned cell phones for this purpose.**

3. All accounts will be audited regularly. Any misuse of the VMS will result in the revocation of access privileges, and/or discipline, up to and including termination.

G. OTHER JURISDICTION DEPARTMENTS' ACCESS TO CAMERA NETWORKS

1. Other jurisdiction departments will have access to cameras within their departments. The City of Wilmington Information Technology (IT) Department will be responsible for facilitating user accounts and limiting access to individual department cameras so that each agency department can only access necessary cameras in their department.

H. CAMERA REGISTRY

1. The camera registry is a voluntary database of business or residential locations that have recorded surveillance. The registrant will have the option to provide contact information, should an incident occur around their provided location, so the police can contact them. This will enable detectives the ability to request videos from businesses or residents who want to participate in the registry. This does not give the Wilmington Police Department access to the video feed.

V. STING Center Facility and Operations

A. MONITORING EMPLOYEES ACCESS

1. Keycard access to the STING Center is limited to STING Center staff, the Training, Technology, and Recruiting Captain, the Investigations Bureau Deputy Chief, and the Chief of Police.

2. All others wishing to access the STING Center will sign in upon being let in and will indicate the date, time in/out, and reason for visit.

B. OPERATING PROCEDURES AND GUIDELINES

1. The STING Center staff will be responsible for the overall control and security of video surveillance systems and maintain a record of the camera locations.

2. The STING Center Supervisor will be responsible for remaining up to date on laws or policies that may affect the monitoring protocol for the Public Safety Cameras. The agency will also follow the video surveillance industry to stay abreast of technology changes and the best practices in the industry.

3. STING Center personnel will be trained in the appropriate use of Public Safety Cameras and shall use the cameras for legitimate police purposes only. Personnel will receive ongoing training as needed.

4. Video monitoring is prohibited where individuals have a reasonable expectation of privacy. If video monitoring is necessary to secure evidence in a criminal investigation and a reasonable expectation of privacy exists, a search warrant shall be obtained prior to the commencement of any monitoring.

5. The cameras will be monitored from the STING Center, or other restricted access location(s) as designated by the agency head or designee. Access to the camera images at remote locations, such as desktop computers, mobile phones, and mobile computer terminals, will be restricted and password protected. Only the agency head or designee may authorize personnel to have access to remote locations.

6. Data obtained and stored will be used exclusively for legitimate law enforcement purposes.

7. Public Safety Camera Network videos can be temporarily, digitally stored, and secured within the VMS by STING Center staff. Videos can be uploaded to the permanent, secure digital storage system for evidentiary purposes by STING Center staff. Only authorized personnel will have access to and be able to retrieve images from Public Safety Cameras.

8. Images obtained through surveillance monitoring or recording will be retained by the department for a length deemed appropriate for monitoring but will not exceed thirty (30) days unless such images are being used for a criminal investigation, training purposes, administrative needs, or existing anticipated Public Records Requests. Images will be automatically overwritten after thirty (30) days (self-purge from the system).

9. Any images retrieved and stored for the above purposes will follow standard evidentiary procedure and/or retention requirements currently in place per agency policy.

10. The release of images will be governed by all applicable open records laws.

11. Retrieval of stored images will be viewed by authorized personnel only. Requests for copies of stored images will be made in writing via email to the main email address utilized by the STING Center.

12. Employees may be subject to discipline if the system is used inappropriately and/or if the information is inappropriately obtained, duplicated, or distributed in violation of this policy. Discipline could include termination.

13. The STING Center shall create and maintain a camera inventory of all cameras placed into service and all other camera activities.

14. The Agency Camera Technician (or designee) and vendor camera technicians shall inspect all cameras regularly.

15. Except under a court order, it is a violation of this Policy to observe or record footage of, locations except those that are in public view, accessible to the public, and where there is no expectation of privacy. Areas where there is a reasonable expectation of privacy include the interior of private premises, such as a home.

16. It is a violation of this Policy to use Public Safety Cameras to harass and/or intimidate any individual or group.

17. It is a violation of this Policy to use Public Safety Camera Network cameras for any personal use.

18. It is a violation of this Policy to use Public Safety Camera Network cameras to infringe upon any Constitutional rights.

VI. Storage and Retrieval of Video Images

A. AGENCY CAMERA STORAGE AND PUBLIC RECORDS

1. Video images recorded with agency cameras will be stored electronically for thirty (30) days. Images will be withheld according to the Public Records Act. Video images will only be released to the public via official Public Records requests in accordance with WPD Written Directive .03.04 – Media Relations related to Public Records requests. Criminal or intelligence investigative video images will not be released

to the public, per the Public Records Act following Federal, State, and Local law. Images from any Homeland Security camera will not be released to the public for any reason.

B. PRIVATE DONOR CAMERAS

1. The decision to record any private donor camera is at the sole discretion of the private donor. Any video images recorded with a private donor camera are the responsibility of the private donor.

C. TRAFFIC CAMERAS

1. The STING Center has access to view the City of Wilmington Traffic & Engineering cameras throughout the jurisdiction.

D. INTERNAL REQUESTS FOR RETRIEVAL OF VIDEO IMAGES

1. Internal requests to review video images shall be made either in writing, via the main email address utilized by the STING Center, or verbally to STING Center staff. If the request is made verbally, the request will be documented by STING Center staff in the current shift's section of the Shift Report. STING Center staff can make the specified video(s) available to officers. The requested video will be housed in a temporary storage sure maintained and secured within the VMS. Requesting employees can review the video themselves and determine evidentiary value. Only STING Center staff will upload permanent video evidence. The retrieval of video images is to be used for law enforcement purposes only, including, but not limited to criminal investigations, training, and/or administrative needs. The person requesting the reproduction of video images is solely responsible for ensuring that the video is maintained properly. Once it has been determined that the video image is no longer needed, it shall be disposed of in the method established for the destruction of records.